IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICES SEIZED PURSUANT TO A CONSENT SEARCH OF A 2007 PONTIAC, CURRENTLY LOCATED AT 4100 N. MULBERRY DRIVE, SUITE 225, KANSAS CITY, MO 64116	Case No. 14-SW-00091-SWH

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Edgar Jones being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been since October of 2009. Prior to ICE-HSI's creation, between 2007 and 2009, I was employed as an Immigration Enforcement Agent (IEA) with the Enforcement and Removal Operations (ERO) component of ICE. I attended the Federal Law Enforcement Training Center (FLETC) at Glynco, Georgia. I completed the ICE Academy, which included training in enforcing Title 8 of the United States Code. I subsequently graduated from the Criminal Investigator Training Program (CITP), which included training in investigating violations of Title 18 of the United States Code. I have a combined total of over five years of conducting

immigration-related investigations, which led to successful prosecutions of violators of Titles 8 and 18 of the United States Code.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched, hereinafter the "Devices" or "electronic devices," are identified below.

Items seized pursuant to a consensual search of a grey 2007 Pontiac Grand Prix, displaying Kansas registration 486 DTI conducted on February 21, 2014:

a. A Dell Optiplex 740 desktop computer tower, serial number HJ07PC1;

b. An HP Compaq desktop computer tower, serial number ZUB4160507;

c. A black LG Tracfone cellular telephone (serial number not visible);

d. A dark grey LG 'smartphone' style cellular telephone (serial number not visible);

e. A San Disk brand USB flash drive (model number not known);

f. A PNY brand USB flash drive (model number not known); and

g. A Sony brand memory stick (1GB of memory, model number not known).

These Devices are currently located at 4100 N. Mulberry Drive, Suite 225, Kansas City, MO 64116.

5. The electronic devices identified in paragraphs 4(a) through 4(g) listed above were all seized pursuant to a consensual search of a grey 2007 Pontiac Grand Prix, displaying Kansas registration 486 DTI. On February 21, 2014, Oscar "Reyes" MATA-Villegas drove this Pontiac Grand Prix to apartment complex at 711 S. Prairie Street, Liberty, Missouri, 64068. Later that same day, MATA-Villegas provided federal agents of Homeland Security

Investigations ("HSI") consent to search his vehicle. Pursuant to the consensual search, HSI seized numerous items from the vehicle, to include the electronic devices identified in paragraphs 4(a) through 4(g) of this affidavit. HSI investigators took these electronic devices to HSI offices located at 4100 N. Mulberry Drive, Suite 225, Kansas City, MO 64116. This affidavit supports an application to search these seized electronic devices.

6. This applied-for warrant would authorize the forensic examination of the electronic devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. I opened this investigation in September of 2013, after a concerned citizen who resides at the apartment complex at 711 S. Prairie Street, Liberty, Missouri, 64068 contacted HSI Kansas City. The complainant advised law enforcement that Apartment 1 in his/her apartment complex had a significant number of Hispanic individuals speaking exclusively Spanish, who were frequently coming in and out of a two bedroom apartment. I know from prior professional training and experience that individuals involved in the transportation of illegal aliens often harbor the illegal aliens at residences within the interior of the United States, and these residences are often used exclusively for the purpose of shielding the illegal aliens from detection. Additionally, as detailed later in this affidavit, as part of my investigation I have been working with a Source of Information ("SOI") who is familiar with both MUJICA and MEDINA. The SOI informed me MUJICA and others were using Apartment 1 as a locus to manufacture fraudulent or counterfeit identification documents.

8. I previously identified the SOI as a subject who could provide information to HSI regarding the activities at the residence located at 711 S. Prairie Street, Apartment 1, Liberty, Missouri, 64068. I contacted this subject, and he/she agreed to serve HSI and other law enforcement agencies as an SOI. Special Agent ("SA") Joseph Espinosa, of the Office of the Inspector General for the Social Security Administration ("SSA-OIG") and I subsequently debriefed the SOI, and he/she stated the following:

a. "Oscar Gomez" is Cesar MUJICA. The SOI stated MUJICA uses the alias Oscar Gomez. He/she also stated MUJICA possesses and operates equipment used to manufacture fraudulent identification documents, such as Lawful Permanent Resident (LPR) cards and Social Security cards. MUJICA also distributes the manufactured fraudulent identification documents to street-level couriers to fulfill orders placed by illegal aliens. The SOI has personally known and associated with MUJICA for over two years, and personally observed MUJICA using the alias Oscar GOMEZ-Gomez when they were stopped by the Ray County, Missouri Sheriff's Office.

9. On October 23, 2013, the SOI personally observed reels of color card printer ribbon and packs of white PVC cards at the residence of the leader, Moises MEDINA, 14536 Beamer Road, Rayville, MO 64084. Later that day, the SOI personally observed reels of color card printer ribbon and packs of white PVC cards at the residence of MUJICA, 711 S. Prairie Street, Apt. 1, Liberty, MO 64068.

10. On November 6, 2013, the SOI advised me that he/she had personally observed the manufacturing equipment at 711 S. Prairie Street, Apartment 1, Liberty, Missouri 64068. The SOI confirmed the location of the manufacturing equipment on November 9, 10, and 13.

11. On November 19, 2013, SA Joseph Espinosa of the Office of the Inspector General for SSA and I met with the SOI, and he/she stated that earlier in the day, he/she had personally seen the equipment used to make fraudulent identification documents inside 711 S. Prairie Street, Apartment 1, Liberty, MO 64068. The SOI showed us several fraudulent identification documents that he/she claimed were manufactured by MUJICA earlier in the day. These included purported Legal Permanent Resident (LPR) cards and Social Security cards. Based on our training and experience, both SA Espinosa and I immediately recognized that these identification documents were fraudulent due to their lack of security features found on the authentic identification documents. The SOI also showed us the packaging material used for delivery: a half of a security envelope, itself folded in half. A distinctive blue pattern was printed on the inside of the security envelope.

12. Late at night on January 30, 2014, the SOI advised that MUJICA had thrown away a white plastic bag containing shredded pieces of fraudulent identity documents in a trash can at a gas station at St. John Avenue and Belmont in Kansas City, Missouri. Early in the morning of January 31, 2014, I responded to the BP brand gas station located at 6201 St John Avenue in Kansas City, Missouri and located the bag in the trash can immediately adjacent to the middle gas pump. The bag contained shredded pieces of suspected fraudulent identification documents, and weighed approximately two pounds. Each piece was approximately the size of a small paper clip, and the shredded pieces were immediately recognizable as fraudulent LPR cards, social security cards, Missouri non-driver's licenses, and Kansas identification cards. Upon further examination, I discovered two reels of depleted color card printer ribbon within the shredded pieces. One reel had images of fraudulent LPR cards visible to my naked eye, and the other had at least one continuous latent fingerprint visible to my naked eye. I subsequently

packaged and sent these items of evidence to the Homeland Security Investigations (HSI) Forensic Laboratory (HSI-FL) and requested latent print examination of the fingerprint(s) on one of the reels of depleted ribbon, as well as the plastic grocery bags. In addition, I requested images of all the fraudulent identification documents produced using these reels, as well as a tally based on type of identity document.

13. According to the SOI, on the night of February 20, 2014, MEDINA instructed Oscar "Reyes" MATA-Villegas, a street-level courier, to enter 711 S Liberty St, Apt. 1, Liberty, MO 64068 and retrieve the cash proceeds of the sales of fraudulent identity documents in order to post bond for Cesar MUJICA at the Wyandotte County, Kansas Sheriff's Department Detention Center. "Reyes" entered via the furthest north window facing west of 711 S Liberty St, Apt. 1, Liberty, MO 64068 and retrieved the cash for bond. MEDINA stated to "Reyes" that he was deeply concerned about the arrest of MUJICA, as he believed the arrest placed the document-making implements and supplies in jeopardy of discovery and seizure.

14. According to the SOI, on the morning of February 21, 2014, "Reyes" attempted to post bond for MUJICA, but was unable to do so due to an immigration detainer lodged on MUJICA. MEDINA instructed "Reyes" to hold on to the cash ($1,400) for safekeeping. MEDINA instructed "Reyes" to meet him in Liberty, Missouri in the area of 711 S Liberty St. "Reyes" did so, and MEDINA instructed him to drive in tandem to 711 S Liberty St. "Reyes" complied. MEDINA drove the black 2006 Chevrolet Yukon SUV and "Reyes" drove the grey 2007 Pontiac Grand Prix.

15. According to the SOI, upon arrival, MEDINA ordered "Reyes" to make entry into Apartment 1 via the same window he entered on the night of February 20, 2014. Law enforcement officers from Homeland Security Investigations and the Office of the Inspector

General for the Social Security Administration were at the location monitoring MEDINA and "Reyes." "Reyes" entered Apartment 1 via a window as instructed by MEDINA. "Reyes" unlocked and opened the front door for MEDINA. MEDINA entered Apartment 1 and according to "Reyes," who was interviewed later by Homeland Security Investigations personnel, "Reyes" and MEDINA placed what was later identified as document-making implements into large black plastic garbage bags and MEDINA instructed "Reyes" to place them in the vehicle operated by "Reyes." Law enforcement observed "Reyes" put large black plastic garbage backs in his vehicle.

16. On the morning of February 21, 2014, HSI Kansas City Group 3 observed MEDINA and "Reyes" carrying items out of 711 S. Prairie Street, Apartment 1, Liberty, MO 64068. SA Lindsey took numerous photographs of MEDINA carrying items out of the apartment. SAs Jose Covarrubias and Brian Psenak contacted MEDINA immediately adjacent to the black 2006 GMC Yukon, displaying Missouri registration 6PR 530, owned by RUIZ-Pineda, but operated by MEDINA. The Yukon was parked in the assigned parking spot for apartment 1. MEDINA identified himself both verbally and by a fraudulent Mexican driver's license as Rodolfo Diaz, and stated that he was unlawfully present in the United States. MEDINA consented, both verbally and in writing to a search of the black 2006 GMC Yukon displaying Missouri registration 6PR 530. MEDINA stated that only his wife, Gabriela Medina (RUIZ-Pineda) could consent to a search of their house at 14536 Beamer Road, Rayville, MO 64084, as she owned the property. Out of an abundance of caution, I sought and obtained a federal search warrant to search the GMC Yukon used by MEDINA. S/As Covarrubias and Psenak administratively arrested MEDINA pursuant to his violation of section 212(a)(6)(A)(i) of the INA and transported him to HSI Kansas City, Missouri.

17. A subsequent fingerprint check revealed that MEDINA had numerous alias names and dates of birth, but was assigned FBI number 184482CB8 and state criminal identification number CA11161312. His criminal history under his FBI number showed that he was assigned alien registration number 076 620 789. Records checks of immigration databases revealed that MEDINA had been previously deported from the US to Mexico. MEDINA was previously convicted in the Superior Court of San Bernardino of forging an official seal.

18. Based on my training and experience, I know that the manufacture of counterfeit identification documents requires various forms of equipment and materials. Computers, printers, scanners, thumb drives, CD Rom disks, DVD disks, hard drives and other electronic storage devices are frequently used in the manufacture of counterfeit identification documents. Additionally, printing materials, card stock, paper, packaging materials, various forms of ink, packaging materials and tape are all integral parts of counterfeit identification manufacturing enterprises.

19. On February 21, 2014, MATA-Villegas consented, both verbally and in writing, to a search of the grey 2007 Pontiac Grand Prix, displaying Kansas registration 486 DTI, including the LG cellular telephones inside. A search of the grey 2007 Pontiac Grand Prix, displaying Kansas registration 486 DTI revealed multiple computers, digital media, printers, color card printers, cellular telephones, white plastic cardstock, finished fraudulent identification documents, and office equipment often used to manufacture fraudulent identity documents (paper cutter and laminator). HSI investigators seized these items and transported them to HSI offices located at 4100 N. Mulberry Drive, Suite 225, Kansas City, MO 64116. The electronic devices seized pursuant to the consensual search of the grey 2007 Pontiac Grand Prix were:

a. A Dell Optiplex 740 desktop computer tower, serial number HJ07PC1;

b. An HP Compaq desktop computer tower, serial number ZUB4160507;

c. A black LG Tracfone cellular telephone (serial number not visible);

d. A dark grey LG 'smartphone' style cellular telephone (serial number not visible);

e. A San Disk brand USB flash drive (model number not known);

f. A PNY brand USB flash drive (model number not known); and

g. A Sony brand memory stick (1GB of memory, model number not known).

All of these items were located in garbage bags. Based on my training and experience, I know that these electronic devices are commonly used as implements to manufacture counterfeit identification documents and I also know that cellular phones are often used to the distribution of counterfeit identification documents. Federal agents of Homeland Security Investigations identified MEDINA and MATA-Villegas as the individuals who broke into the residence at 711 S. Prairie Street, Apartment 1, Liberty, MO 64068, who, when they exited the apartment, held garbage bags that appeared to contain items and thereafter they put these bags into the grey 2007 Pontiac Grand Prix.

20. On February 21, 2014, at approximately 1400 hours, HSI Kansas City SAs Ken Lovesee and James Taylor contacted MEDINA's spouse, RUIZ-Pineda, at her place of employment at 1 Armour Road in Kansas City, Missouri. RUIZ-Pineda consented, both verbally and in writing to a search of her house at 14536 Beamer Road, Rayville, MO 64084, as well as her rented storage unit (number 1009) located at Star Storage, 1913 W. Jesse James Road, in Excelsior Springs, Missouri. SAs Lovesee and Taylor accompanied RUIZ-Pineda to her house.

21. On February 21, 2014, at approximately 1405 hours, HSI Kansas City SAs Lovesee and Taylor advised SAs Benjamin Gatrost and Joseph Stewart that the Beamer Road house was unlocked and that RUIZ-Pineda authorized their entry prior to her arrival. SAs Gatrost and Stewart subsequently seized three desktop computer towers, various forms of digital media, two rifles and ammunition, several new and used reels of color card printer ribbon, a suspected fraudulent Arkansas driver's license, number 999027558, and 300 blank white plastic cards from the house. SA Jones subsequently inspected the used reels of color card printer ribbon, and could see images of fraudulent identity documents, such as LPR cards, with my naked eye. The electronic devices that were seized from the residence located at 14536 Beamer Rd, Rayville, Missouri 64084 include the following:

a. HP Pavillion desktop computer tower, serial number MXX2390QVG;

b. Dell desktop computer tower, serial number JX1Y421;

c. eMachines desktop computer tower, serial number PTNBA020019390CE6E2400;

d. PNY brand thumb drive; and

e. CDs and DVDs.

Based on my training and experience and conversations that I have had with other investigators, I know that all of the electronic devices seized from the residence at 14536 Beamer Rd, Rayville, Missouri 64084 are commonly used during the manufacture of counterfeit identification documents.

22. On February 21, 2014, at approximately 1715 hours, SAs Lovesee, Taylor, Gatrost, and Stewart conducted a consensual search of the rented storage unit, number 1009, at Star Storage, 1913 W. Jesse James Road, Excelsior Springs, Missouri 64024. These federal

agents seized a color card printer with its software, used reels of color card printer ribbon, various forms of digital media, a black cellular telephone missing its memory card, office supplies commonly used to manufacture fraudulent identification documents (razor blades and laminate materials), and two color copies of a Lawful Permanent Resident (LPR) card (current version). RUIZ-Pineda stated that she knew the woman who was issued that LPR card. SA Jones subsequently inspected the used reels of color card printer ribbon, and could see images of what appeared to be fraudulent identity documents, such as LPR cards, with my naked eye. The electronic devices that were seized during the consensual search of storage unit number 1009 include the following:

a. Black cellular telephone missing its memory card;

b. Digital media storage USB 2.0 flash drive; and

c. CDs and DVDs.

Based on my training and experience and conversations that I have had with other investigators, I know that all of these electronic devices are commonly used during the manufacture of counterfeit identification documents and I know cellular phones are commonly used in the trafficking of counterfeit identification documents.

23. On February 21, 2014, I applied for and obtained federal search warrants 14-SW-00055 and 14-SW-00056 for 711 S. Prairie Street, Apartment 1, Liberty, MO 64068 and the black 2006 GMC Yukon displaying Missouri registration 6PR 530. At approximately 2145 hours, HSI Kansas City SAs Tim Ditter and Jose Covarrubias, and I searched the apartment and vehicle. SAs Covarrubias and Ditter seized approximately 24 pounds of used reels of color card printer ribbon, office supplies used to manufacture fraudulent identity documents (paper cutters and a laminator), a shredder, and about eight pounds of shredded pieces of suspected fraudulent

identification documents from the apartment. SA Jones and I subsequently inspected the used reels of color card printer ribbon, and I could see images of fraudulent identity documents, such as LPR cards, with my naked eye. The electronic devices that were seized during the execution of the search warrant of the residence located at 711 S. Prairie Street, Apartment 1, Liberty, Missouri, 64068, include:

a. CDs & DVDs;

b. Kodak camera;

c. Nikon Coolpix camera;

d. Olympus camera;

e. Casio Exilim camera;

f. Verizon Samsung flip-style cellular telephone;

g. HTC cellular telephone (broken screen);

h. White Samsung cellular telephone;

i. Sprint HTC cellular telephone;

j. Seagate 1TB hard drive; and

k. Dell Inspiron One computer, serial number 4RFJSM1.

Based on my training and experience and conversations that I have had with other investigators, I know that all of these electronic devices are commonly used during the manufacture of counterfeit identification documents and I know cellular phones are commonly used in the trafficking of counterfeit identification documents.

24. On March 4, 2014, I swore to a criminal complaint charging MEDINA with being an illegal alien in possession of a firearm. MEDINA's initial appearance on this charge was on March 6, 2014.

25. On March 20, 2014, a federal grand jury returned an indictment charging four defendants with a total of six counts and a forfeiture allegation. *See* Case Number 14-00072-DW, ECF Docket Entry Number 13. The defendants identified in the indictment are: Eriberto Moises Medina-Aranda; Ceasar Mujica-Aranda; Bernardino Bautista-Hernandandez, and Ulises Montiel-Lazcano. All of the defendants are charged with Counts Five and Six. Count Five alleges that the defendants conspired to produce false identification documents, in violation of 18 U.S.C. §§ 1028(a)(1), (b)(1)(A)(i), (b)(5), and (f). Count Six alleges that the defendants aided and abetted each other in the efforts to counterfeit documents used as evidence of authorized stay or employment in the United States, in violation of 18 U.S.C. § 1546. Count Four charges MEDINA and MUJICA with possessing identification document-making implements, in violation of 18 U.S.C. § 1028(a)(5), (b)(1)(C), (b)(5), and § 2. Counts One through Three relate solely to offenses allegedly committed by MEDINA.

26. Based on my training and experience and based on my investigation of this case, I know individuals who want to purchase counterfeit identification documents often send a text messages from their cellular telephones to the cellular telephone of a street-level courier who sales fraudulent identity documents. The text messages often contain the personal identifiers of the customers, and an electronic photograph of each customer is often attached. The street-level courier typically forwards this text message to the operator of the document-making implements, who then transcribes the identifiers, but electronically transfers the customer photo from his cellular telephone to the computer being used to manipulate the electronic templates for the

fraudulent ID documents. These electronic templates are often located on digital media, such as external hard drives, flash/thumb drives, DVDs, and CDs. The SOI has indicated that this form of trafficking was frequently used by the conspirators charged in the aforementioned indictment. I have also conducted consensual searches of phones owned by MUJICA and BAUTISTA-Hernandez and confirmed that they both had cellular telephones with text messages containing personal identifiers of apparent customers who were purchasing counterfeit identification documents.

27. This affidavit supports an application to search each of the electronic devices that were found during the consensual search of the grey 2007 Pontiac Grand Prix. Based on my training and experience and conversations that I have had with other investigators, I know that all of the electronic devices identified in paragraphs 4(a) through 4(g) of this affidavit are devices that are commonly used during the manufacture of counterfeit identification documents and some of the items such as the cellular phones are commonly used to aid the trafficking of counterfeit identification documents.

28. The Devices are currently in the lawful possession of the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). The Devices are currently in storage at 4100 N. Mulberry Drive, Suite 225, Kansas City, MO 64116. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI. The Devices were seized by HSI following the execution of a search warrant of the residence located at 711 S. Prairie Street, Apartment 1, Liberty, Missouri, 64068.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (GPS) technology for determining the location of the device.

b. Removable storage media: includes various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of

four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on my training and experience, I know that computers, cameras, cellular phones, and digital media storage devices are commonly used in the manufacture and trafficking of counterfeit identification documents.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

35. Because it appears that the Devices were used to further a criminal conspiracy to produce counterfeit identification documents, it is highly likely that the Devices in question will be subject to criminal or civil forfeiture.

SEARCH METHODOLOGY TO BE EMPLOYED

36. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

CONCLUSION

37. I submit that this affidavit supports probable cause to believe that a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B will discover evidence of various federal offenses related to the production and distribution of counterfeit identification documents, including documents prescribed by statute or regulation to be used as evidence of authorized stay or employment in the United States.

Respectfully submitted,

Edgar Jones
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on April 8th, 2014:

SARAH W. HAYS
CHIEF UNITED STATES MAGISTRATE JUDGE